Typical entanglement of stabilizer states

Graeme Smith[*] and Debbie Leung[†]

Institute for Quantum Information, Caltech 107–81, Pasadena, CA 91125, USA
(Dated: February 1, 2008)

How entangled is a randomly chosen bipartite stabilizer state? We show that if the number of qubits each party holds is large the state will be close to maximally entangled with probability exponentially close to one. We provide a similar tight characterization of the entanglement present in the maximally mixed state of a randomly chosen stabilizer code. Finally, we show that typically very few GHZ states can be extracted from a random multipartite stabilizer state via local unitary operations. Our main tool is a new concentration inequality which bounds deviations from the mean of random variables which are naturally defined on the Clifford group.

I. INTRODUCTION

Randomly chosen states and subspaces play a central role in the study of quantum information. For example, the consideration of random stabilizer codes played a crucial role in one of the first proofs that there exist good quantum correcting codes [15], as well as much of the early understanding of entanglement distillation and quantum channel capacities [2, 11, 28]. More recently, through an improved understanding of the typical properties of randomly chosen quantum states, expressions for many capacities of quantum channels [7, 8, 9, 27, 33], several advances in cryptography [4, 17, 18], and an emerging understanding of quantum correlations in high dimensional systems [19] have all been attained.

Perhaps the property of quantum states that it is most important to understand is entanglement. Entanglement is an essential resource in quantum information which nevertheless remains quite poorly understood in general. Even in the asymptotic limit it is difficult to characterize the entanglement in a bipartite mixed state. Indeed, such fundamental quantities as the entanglement of formation, E_F, and the distillible entanglement, E_D, are unknown in all but a few examples (see, e.g.,[24, 32, 34]). It has, however, proved possible to find tight bounds on the typical E_F and E_D of a random mixed state, $\rho_U = \frac{1}{r} \sum_{i=1}^{r} U|i\rangle\langle i|U^\dagger$ of rank 2^k, both local dimensions roughly $2^n \gg 1$, and where U is distributed according to the unitarily invariant measure (i.e., the Haar measure) on $\mathbb{U}(d_A d_B)$[19]. The surprising result is that with high probability, ρ_U has $E_F \approx n$ and $E_D \leq n - \frac{k}{2}$ which implies that a typical ρ_U of high rank ($2^k \approx 2^{2n}$) has near maximal entanglement of formation while having distillable entanglement which is exponentially smaller, implying either an extreme irreversibility in the creation of ρ_U or a near maximal violation of the conjecture of E_F's additivity [26]. While this dichotomy is quite strik-

ing, its physical and computational significance are not at all clear – no constructions of such extreme states are known, and the generation of a state distributed like ρ_U would require exponential resources. Characterizing the typical entanglement of random states whose distribution *can* be generated efficiently is thus crucial to understanding whether this irreversibility is a fact of nature or merely a mathematical curiosity.

In this paper, we characterize the typical entanglement for just such a distribution – the uniform distribution on the set of stabilizer states, which can be generated efficiently using the random walk based algorithm of [10]. Stabilizer states are relevant to almost all known quantum error correcting codes, and as such it is hoped that a characterization of their typical entanglement properties will not only shed light on the irreversibility question mentioned above, but also point us towards better codes. Furthermore, since a highly entangled multipartite stabilizer state is the fundamental resource in the one-way model of quantum computation [25], a deeper understanding of such states may elucidate the role played by entanglement in quantum computations.

The bipartite entanglement of stabilizer states has previously been explored in [1, 3, 14], with the result that any such state can be transformed by local unitaries (i.e., it is LU-equivalent) to a tensor product of EPR pairs and (possibly classically correlated) local states. An expression for the number of EPR pairs that can be extracted from any particular stabilizer state in terms of the structure of its stabilizer group was also found. Our contribution is to estimate the expectation of this expression for a random stabilizer group, and provide an exponential bound on deviations from this estimate. Shortly after this work first appeared, results for the case of pure stabilizer states were presented in [5].

In contrast to a rank 2^k state with a Haar-induced distribution, we find that a random $2^n \times 2^n$ rank 2^k stabilizer state has $E_F = E_D \approx n - \frac{k}{2}$. That E_D and E_F must coincide is clear, since any stabilizer state is LU-equivalent to the tensor product of EPR pairs and a separable state. It is facinating, however, that the value they take is essentially maximal – a stabilizer state of rank 2^k can have

at most $2n - k$ pure qubits, and in a typical such state each of these is half of an EPR pair.

In addition to these results on bipartite entanglement, we are able to characterize the typical number of GHZ states that can be extracted via local unitaries from a random multipartite stabilizer state. Unlike EPR pairs, which are abundant in a random bipartite state, GHZ-equivalent states are quite uncommon. For example, we find that for a pure m-partite state in which all m systems are of size roughly n qubits, in the limit of large n the expected number of GHZ states that can be extracted via local unitaries is close to zero, and that significant deviations from this mean are unlikely.

We will concentrate on the case where all of our systems have asymptotically equal numbers of qubits (e.g., bipartite systems of $n_A + n_B$ qubits with $n_A = n$ and $n_B = n + O(\log n)$), both because this case is likely the most useful in terms of applications and because it is exactly where standard Markov-type arguments break down. For instance, in the case of bipartite stabilizer states a straightforward Markov inequality argument can be used to give bounds on deviations of entanglement from its mean of the form $\frac{1}{2^{n_A - n_B}}$, but when $n_A = n$ and $n_B = n + O(\log n)$ this bound is quite weak, scaling like $\frac{1}{n^{O(1)}}$. Using a new concentration inequality, we are able to provide exponential bounds in this regime.

Our main tool throughout is Theorem II.1, which captures the notion of measure concentration on the Clifford group. In particular, this Theorem is a quantitative version of the intuitively obvious observation that a slowly varying function on the Clifford group won't deviate significantly from its mean. The result is quite general, and we expect it will prove useful in further analyses of the entanglement of stabilizer states, as well as the analysis of stabilizer codes.

The paper is organized as follows. In Section II we present a bound on deviations from the mean of random variables on the Clifford group. In Section III we use this inequality to characterize the typical entanglement in a pure bipartite stabilizer state, in section IV we study pure multipartite states, while in Section V we turn our attention to mixed bipartite stabilizer states. Section VI contains a few comments on other applications of our inequality as well as some open questions.

We use the following conventions throughout. log and exp are always base 2. The Pauli group on n qubits is denoted by $\mathcal{P}_n$. An abelian subgroup of $\mathcal{P}_n$ with 2^{n-k} elements will typically be called S^{n-k} and have generators $\{S_i\}_{i=1}^{n-k}$. Two elements of $\mathcal{P}_n$, P_1 and P_2, either commute or anticommute with the commutation relation $P_1 P_2 = (-1)^{\omega(P_1, P_2)}$ serving as a definition for $\omega(P_1, P_2)$. Angle brackets will denote the group generated by the elements they enclose, so that, e.g., $S^{n-k} = \langle S_i \rangle_{i=1}^{n-k}$. The dimension of a subgroup of $\mathcal{P}_n$ is the logarithm of the number of elements in the group, so that $\dim S^{n-k} = n - k$. We say that $|\psi\rangle$ is stabilized by U when $U|\psi\rangle = \psi$, and call $|\psi\rangle$ a stabilizer state on n qubits if it is simulataneously stabilized by all elements of a maximal Abelian subgroup (S) of the Pauli group on n qubits. A mixed stabilizer state of rank 2^k is the maximally mixed state on the subspace stabilized by an Abelian subgroup $S \subset \mathcal{P}_n$ of size 2^{n-k}, or equivalently is the maximally mixed state on the stabilizer code defined by S.

The Clifford group on n qubits is denoted by $\mathcal{C}_n$ and its elements are typically called c. A real valued function, F, on a metric space (X, d) is called η-Lipschitz if $|F(x) - F(y)| \le \eta d(x, y)$ for all $x, y \in X$. $\mathbb{E}$ denotes an expectation value, while $g \in_R G$ is a random variable distributed uniformly on G.

II. A CONCENTRATION INEQUALITY ON THE CLIFFORD GROUP

The notion of measure concentration is a generalization of the basic fact from probability theory that the empirical mean of many i.i.d. random variables, $\frac{1}{N} \sum_{i=1}^{N} X_i$, tends to be very close to the mean of the underlying distribution. The point is that not only the empirical mean of a large number of random variables, but *any* function which depends in a sufficiently smooth way on a large number of fairly independent random variables will tend to be roughly constant. The imprecision of of the previous sentence is a reflection of the broad range of problems this idea can be applied to – one's definition of "fairly independent" or "roughly constant" depends on the particular question under consideration [20, 30, 31]. To make precise the notion of a smooth function on the Clifford group, we must first introduce a notion of distance between two elements of the group. One natural candidate is an analogue of the Hamming distance on the set of binary strings. In particular, for some fixed set of generators of $\mathcal{P}_n$, $\{S_i\}_{i=1}^{2n}$, we let the $\{S_i\}$-distance between $c_1, c_2 \in \mathcal{C}_n$ be the number of generators on which c_1 and c_2 disagree (ignoring differences in phase),

$$d_{\{S_i\}}(c_1, c_2) = \# \left\{ i \middle| c_1 S_i c_1^\dagger \ne c_2 S_i c_2^\dagger \right\},$$

and choose the smallest such value over all generating sets of $\mathcal{P}_n$:

$$d(c_1, c_2) = \min_{\{S_i\}} d_{\{S_i\}}(c_1, c_2). \tag{1}$$

That this defines a metric is shown in section IV.

Our "smooth" functions will be those which are 1-Lipschitz. That is, we will study deviations from the mean of real functions F on $\mathcal{C}_n$ such that $|F(c_1) - F(c_2)| \le d(c_1, c_2)$. The precise meaning of the claim that they are "roughly constant" is given by the following theorem.

Theorem II.1 *Let F be a 1-Lipschitz function on $(\mathcal{C}_n, d)$ and $c \in_R \mathcal{C}_n$ be a uniformly distributed random variable. Then*

$$P\left(|F(c) - \mathbb{E}F(c)| > \delta\right) < 2 \exp\left[-\frac{\delta^2}{64n}\right].$$

We will prove this theorem, which is quite similar to a result of Maurey for the symmetric group [22], by using a result of [20] that characterizes concentration on a finite metric space. In particular, we say that a metric space (X, d_X) has length at most L if there exists an increasing sequence of partitions (i.e, a filtration) of X,

$$\{X\} = \chi^0 \subset \chi^1 \cdots \subset \chi^m = \{\{x\}\}_{x \in X}$$

and real numbers $a_0, \ldots, a_m$ with $\sum_{i=0}^m a_i^2 = L^2$ such that if $\chi^i = \{A_j^i\}_{j=1 \ldots r_i}$ and $A_j^i, A_k^i \subset A_p^{i-1}$ there exists a bijection $\phi_{ip}^{jk} : A_j^i \to A_k^i$ that satisfies $d_X(x, \phi_{ip}^{jk}(x)) \leq a_i$ (Fig. (1) may help elucidate this fairly clumsy definition). A concentration inequality is then given by the following.

Theorem II.2 *(4.2 of [20]) Let (X, d_X) be a finite metric space of length at most L and let P be the normalized counting measure on X. Then, for every 1-Lipschitz function F on (X, d_X) and every $\delta \geq 0$*

$$P\left(\{F \geq \mathbb{E}F + \delta\}\right) \leq \exp\left[-\delta^2/2L^2\right].$$

Theorem II.1 is an immediate consequence of the following theorem.

Theorem II.3 *The length of $(\mathcal{C}_n, d)$ is at most $\sqrt{32n}$.*

Proof Let $\{S_i\}_{i=1}^{2n}$ be a set of generators for $\mathcal{P}_n$ such that for $t \in \{1, \ldots, n\}$, S_{2t-1} and S_{2t} anticommute and all other pairs of generators commute. We choose our filtration of $\mathcal{C}_n$ to be

$$\chi^k = \{A_{P_1 P_2 \ldots P_k}^k\},$$

where $\{P_i\}_{i=1}^k$ are independent elements of $\mathcal{P}_n$ such that $\omega(P_i, P_j) = \omega(S_i, S_j)$ and

$$A_{P_1 P_2 \ldots P_k}^k = \{c \in \mathcal{C}_n | c S_i c^\dagger = P_i \text{ for } i = 1 \ldots k\}.$$

Now we need to find bijections

$$\phi_{P_1 \ldots P_{k-1}}^{PQ} : A_{P_1 P_2 \ldots P_{k-1} P}^k \to A_{P_1 P_2 \ldots P_{k-1} Q}^k.$$

We first consider the case where Q is independent of $\{P_1, \ldots, P_{k-1}, P\}$ and k is even. Since both P and Q anticommute with P_{k-1} and commute with $\{P_i\}_{i=1}^{k-2}$, we can always find T_1 and T_2 such that the ordered lists

$$\{P_1, \ldots, P_{k-1}, P, Q, T_1\}$$

and

$$\{P_1, \ldots, P_{k-1}, Q, P, T_2\}$$

have the same commutation relations and are independent generators for the same group. In particular, given any T_1 which commutes with $\{P_i\}_{i=1}^{k-2}$ and is independent of

$$\{P_1, \ldots, P_{k-1}, P, Q\}$$

we can simply choose

$$T_2 = T_1$$

if $\omega(P, T_1) = \omega(Q, T_1)$ and

$$T_2 = P_{k-1} T_1$$

if $\omega(P, T_1) \neq \omega(Q, T_1)$. This allows us to extend both sets to generators of $\mathcal{P}_n$ with the *same* $P_{k+3}, \ldots P_{2n}$. That is,

$$S^P = \{S_i^P\}_i = \{P_1, \ldots, P_{k-1}, P, Q, T_1, P_{k+3}, \ldots, P_{2n}\}$$

and

$$S^Q = \{S_i^Q\}_i = \{P_1, \ldots, P_{k-1}, Q, P, T_2, P_{k+3}, \ldots, P_{2n}\}$$

both generate the Pauli group and have the same commutation relations. As a result, there is an element of the Clifford group $c_{PQ} \in \mathcal{C}_n$ such that

$$c_{PQ} S_i^P c_{PQ}^\dagger = S_i^Q$$

and choosing

$$\phi_{P_1 \ldots P_{k-1}}^{PQ}(c_1) = c_1 c_{PQ}$$

gives us

$$d(c_1, \phi_{P_1 \ldots P_{k-1}}^{PQ}(c_1)) \leq d_{\{c_1^\dagger S_i^P c_1\}}(c_1, \phi_{P_1 \ldots P_{k-1}}^{PQ}(c_1)) \leq 3.$$

If k is odd and Q is independent of

$$\{P_1, \ldots, P_{k-1}, P\}$$

we can make a similar argument. In particular, if $PQ = -QP$ (i.e., $\omega(P, Q) = 1$), we can immediately extend

$$\{P_1, \ldots, P_{k-1}, P, Q\}$$

and

$$\{P_1, \ldots, P_{k-1}, Q, P\}$$

to

$$S^P = \{S_i^P\}_i = \{P_1, \ldots, P_{k-1}, P, Q, P_{k+2}, \ldots, P_{2n}\}$$

and

$$S^Q = \{S_i^Q\}_i = \{P_1, \ldots, P_{k-1}, Q, P, P_{k+2}, \ldots, P_{2n}\},$$

so that S^P and S^Q have the same commutation relations and are different in only two entries. Choosing

$$\phi_{P_1 \ldots P_{k-1}}^{PQ}(c_1) = c_1 c_{PQ},$$

where again

$$c_{PQ} S_i^P c_{PQ}^\dagger = S_i^Q,$$

we find

$$d(c_1, \phi^{PQ}_{P_1 \dots P_{k-1}}(c_1)) \leq 2.$$

If P and Q commute, there are T_1 and T_2 such that

$$\{P_1, \dots, P_{k-1}, P, Q, T_1, T_2\}$$

are independent, and satisfy

$$\begin{aligned}
T_j P_i &= P_i T_j \\
Q T_1 &= T_1 Q, \\
Q T_2 &= -T_2 Q, \\
P T_1 &= -T_1 P, \\
P T_2 &= T_2 P,
\end{aligned}$$

so that there are

$$S^P = \{S_i^P\}_i = \{P_1, \dots, P_{k-1}, P, Q, T_1, T_2, P_{k+4} \dots, P_{2n}\}$$

and

$$S^Q = \{S_i^Q\}_i = \{P_1, \dots, P_{k-1}, Q, P, T_2, T_1, P_{k+4}, \dots, P_{2n}\}$$

with the same commutation relations. Once again we use c_{PQ} such that

$$c_{PQ} S_i^P c_{PQ}^\dagger = S_i^Q$$

to define $\phi^{PQ}_{P_1 \dots P_{k-1}}$ and find that this time,

$$d(c_1, \phi^{PQ}_{P_1 \dots P_{k-1}}(c_1)) \leq 4.$$

When $Q \in \langle P_1, \dots, P_{k-1}, P \rangle$ and k is even, the requirements that $Q \notin \langle P_1, \dots, P_{k-1} \rangle$, $\omega(P_i, Q)=0$ for $i=1, \dots, k-2$, and $\omega(P_{k-1}, Q)=1$ imply that the only choice for Q that is not equal to P is just $Q \propto PP_{k-1}$, so we can let

$$S^P = \{P_1, \dots, P_{k-1}, P, P_{k+1} \dots, P_{2n}\}$$

and

$$S^Q = \{S_i^Q\}_i = \{P_1, \dots, P_{k-1}, Q, P_{k+1}, \dots, P_{2n}\}$$

and proceed as above, with the result that

$$d(c_1, \phi^{PQ}_{P_1 \dots P_{k-1}}(c_1)) \leq 1.$$

If k is odd and $Q \in \langle P_1, \dots, P_{k-1}, P \rangle$, we find that Q can only satisfy the required commutation relations and belong to $\langle P_1, \dots, P_{k-1}, P \rangle$ if $Q \propto P$, so in this case we find that
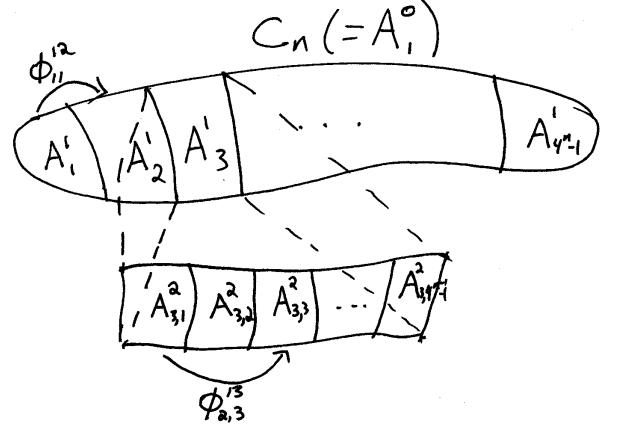

FIG. 1: Finding the length of $\mathcal{C}_n$. We construct an increasing sequence of partitions of $\mathcal{C}_n$, $\{\mathcal{C}_n\} = \chi^0 \subset \chi^1 \cdots \subset \chi^{2n} = \{\{c\}\}_{c \in \mathcal{C}_n}$, such that any pair of sets in a partition which belong to the same set in the preceding partition have a bijection, ϕ, that satisfies $d(c, \phi(c)) \leq 4$. Our filtration contains $2n$ partitions, so our length is then $\sqrt{32n}$.

$$d(c_1, \phi^{PQ}_{P_1 \dots P_{k-1}}(c_1)) = 0$$

(recalling that we equate Clifford group elements which differ only by phases).

Collecting the various cases, we see that we can find the bijections we require with $a_k \leq 4$, so that the length of $\mathcal{C}_n$ is no more than

$$L = \sqrt{\sum_{k=1}^{2n} a_k^2} = \sqrt{32n}.$$

$\square$

III. PURE BIPARTITE STATES

Recently, [14] studied the entanglement of a bipartite stabilizer state in terms of the structure of its stabilizer group. Their result can be summarized as follows.

Theorem III.1 *(Result 1 of [14]) Let $|\psi_{AB}\rangle$ be a pure bipartite stabilizer state with stabilizer S. Then, $|\psi\rangle$ is LU-equivalent to*

$$E(|\psi_{AB}\rangle) = \frac{1}{2} \left[\dim S - \dim(S_{\hat{A}} + S_{\hat{B}}) \right] = n_A - \dim S_{\hat{B}} \tag{2}$$

EPR pairs, where $S_{\hat{A}} = \{g \in S | g = I_A \otimes g_B\}$ and $S_{\hat{B}} = \{g \in S | g = g_A \otimes I_B\}$.

Using this theorem, we will investigate the *average* entanglement of a stabilizer state, then strengthen our results to statements about *typical* states using Theorem II.1. We begin with the following lower bound.

Theorem III.2 *Let $|\psi\rangle$ be uniformly distributed on the set of stabilizer states on AB, where A contains n_A qubits and B has n_B qubits and $n_A \geq n_B$. Then*

$$\mathbb{E}[S(\psi_A)] \geq n_B - \frac{2^{n_B}}{2^{n_A}},$$

where $\psi_A = \mathrm{Tr}_B |\psi_{AB}\rangle\langle\psi_{AB}|$ and $S(\psi_A) = -\mathrm{Tr}\,\psi_A \log \psi_A$ is the von Neumann entropy of ψ_A.

Proof We use a result of [21] for the average subsystem purity of a state uniformly distributed over the entire Hilbert space AB, together with a result of [10] which implies that the average over stabilizer states takes the same value. In particular, in [35] it was shown that if $|\varphi\rangle$ is a uniformly distributed pure state on AB,

$$\mathbb{E}\,\mathrm{Tr}\,\varphi_A^2 = \frac{2^{n_A} + 2^{n_B}}{2^{n_A + n_B} + 1},$$

where the expectation is with respect to the uniform measure on all states in AB. Furthermore, the observation of [10] that a so-called *bilateral Clifford twirl* is equivalent to a bilateral full twirl implies that the average purity of a random stabilizer state has the same value. That is,

$$\mathbb{E}\,\mathrm{Tr}\,\psi_A^2 = \frac{2^{n_A} + 2^{n_B}}{2^{n_A + n_B} + 1},$$

where the expectation is with respect to the uniform distribution on *stabilizer states*. To complete the proof, we use the fact that $-\log\mathrm{Tr}\,\rho^2 \leq S(\rho)$ together with the concavity of the log function to conclude

$$
\begin{aligned}
\mathbb{E}S(\psi_A) &\geq -\mathbb{E}\log\mathrm{Tr}\,\psi_A^2 \\
&\geq -\log\mathbb{E}\,\mathrm{Tr}\,\psi_A^2 \\
&\geq \log\left[\frac{2^{n_A+n_B}+1}{2^{n_A}+2^{n_B}}\right] \\
&\geq n_B - \frac{2^{n_B}}{2^{n_A}}.
\end{aligned}
$$

$\square$

We will also need the following lemma, whose proof depends on a more general lemma of Section IV.

Lemma III.3 *As a function of $c \in \mathcal{C}_{n_A+n_B}$, the entanglement of $|\psi\rangle = c|0\rangle^{\otimes(n_A+n_B)}$ is 1-Lipschitz with respect to the metric defined in Eq (1).*

Proof Using Eq. (2) together with Lemma IV.4, which is proved below, immediately implies the result. $\square$

Theorem III.2, which estimates the average entanglement of a bipartite stabilizer state, can be combined with this evaluation of the Lipschitz constant of the bipartite entanglement of stabilizer state $|\psi\rangle = c|0\rangle^{\otimes(n_A+n_B)}$ to yield a characterization of the typical entanglement in such a state. That is, we can use these to prove Theorem III.4.

Theorem III.4 *Let $|\psi\rangle$ be uniformly distributed on the set of stabilizer states on AB, where A contains n_A qubits and B has n_B qubits and $n_A \geq n_B$. Then the probability of the entanglement of $|\psi\rangle$ deviating from its mean is given by*

$$P\left(S(\psi_A) < \mathbb{E}[S(\psi_A)] - \delta\right) \leq \exp\left[-\frac{\delta^2}{64(n_A+n_B)}\right],$$

where $\psi_A = \mathrm{Tr}_B |\psi_{AB}\rangle\langle\psi_{AB}|$ and $S(\psi_A) = -\mathrm{Tr}\,\psi_A \log \psi_A$ is the von Neumann entropy of ψ_A. In particular, letting $n_A = n + \alpha \log n \geq n = n_B$, $\delta = n\epsilon$, and considering $n \geq 2/\epsilon$ leads to

$$P\left(S(\psi_A) < n(1-\epsilon)\right) \leq \exp\left[-\frac{n\epsilon^2}{512}\frac{2n}{2n+\alpha\log n}\right].$$

Proof of Theorem III.4 From Theorem II.1 and Lemma III.3, we can immediately conclude that

$$P\left(S(\psi_A) < \mathbb{E}S(\psi_A) - \delta\right) \leq \exp\left[-\frac{\delta^2}{64(n_A+n_B)}\right].$$

From Theorem III.2 we know that $\mathbb{E}[S(\psi_A)] \geq n_B - \frac{2^{n_B}}{2^{n_A}}$, so that

$$P\left(S(\psi_A) < n - \frac{1}{n^\alpha} - n\epsilon/2\right) \leq \exp\left[-\frac{n\epsilon^2}{256}\frac{n}{2n+\alpha\log n}\right],$$

which leads to

$$P\left(S(\psi_A) < n(1-\epsilon)\right) \leq \exp\left[-\frac{n\epsilon^2}{512}\frac{2n}{2n+\alpha\log n}\right].$$

$\square$

IV. PURE MULTIPARTITE STATES

The results of the previous section have immediate consequences for the number of GHZ states that can be LU-extracted from a random stabilizer state. In particular, we find the following theorem.

Theorem IV.1 *Let $|\psi_m\rangle$ be a state uniformly distributed on the set of pure m-partite stabilizer states with each party holding n qubits, and where $m \geq 4$. Then if for every $4 \leq m' \leq m$ we let $\Delta^{m'}(|\psi_m\rangle)$ denote the maximal number of m'-GHZ states, $\frac{1}{\sqrt{2}}(|0\rangle^{\otimes m'} + |1\rangle^{\otimes m'})$, that can be extracted from $|\psi_m\rangle$ via unitaries which act locally (with respect to a partition of the m parties into m' groups),*

$$P\left(\Delta^m(|\psi_m\rangle) > \epsilon n\right)$$
$$\leq \exp\left[-\lfloor m/2 \rfloor n\frac{\epsilon^2}{512}(1-1/\lfloor m/2 \rfloor)^2(1-1/m)\right]$$

and

$$P\left(\Delta^{m'}(|\psi_m\rangle) > \epsilon n\right) \leq \exp\left[-n\frac{\epsilon^2}{64}\frac{1}{m}\right].$$

Proof We first consider the case where $m' = m$. Let $k = \lfloor m/2 \rfloor$, B denote parties 1 through k and A denote the rest, and consider the number of EPR pairs with respect to the $A|B$ partition that can be extracted from $|\psi_m\rangle$ via local unitaries on A and B. Supposing $\Delta^m(|\psi_m\rangle) = g$, we can see that the total number of EPR pairs that can be LU-extracted between A and B is no larger than $kn - (k-1)g$ as follows. First notice that local unitaries do not alter the local entropies of A and B, so that the number of EPR pairs A and B can extract is no more than $S(B)$. However, the kg qubit support of B's part of the g GHZ states contains only g bits of entropy, since the reduced state on these qubits is of the form $\left(\frac{1}{2}|0\rangle\langle 0|^{\otimes k} + \frac{1}{2}|1\rangle\langle 1|^{\otimes k}\right)^{\otimes g}$. B's remaining $kn - kg$ qubits can have a maximum of $kn - kg$ bits of entropy, leading us to conclude that $S(B) \leq kn - kg + g$.

Letting $\alpha = (m - 2\lfloor m/2 \rfloor)(n/\log n)$ and using Theorem III.4 we thus find the probability that $\Delta^m(|\psi_m\rangle) > \epsilon n$ is no larger than

$$P\left(S(\psi_B) < kn - (k-1)n\epsilon\right) \leq \exp\left[-\frac{kn\epsilon^2}{512}(1-1/k)^2\frac{2kn}{mn}\right].$$

Similarly, for $4 \leq m' < m$, let B denote the three smallest groups in our partition and let k be the number of parties in B. Once again, if $\Delta^{m'}(|\psi_m\rangle) > \epsilon n$, the number of EPR pairs that can be extracted between A and B can be no larger than $kn - (k-1)n\epsilon$. Theorem III.4 can then be used, this time with $\alpha = (m - 2k)(n/\log n)$, to show that

$$P\left(S(\psi_B) < kn - (k-1)n\epsilon\right) \leq \exp\left[-\frac{kn\epsilon^2}{512}(1-1/k)^2\frac{2kn}{mn}\right].$$

The expressions in the theorem are obtained by substituting the values for k and in the case of $m' < m$ using the fact that $k \geq 3$. $\square$

We cannot understand the entanglement of a tripartite stabilizer state by simply considering the bipartite entanglement of various partitions. In this case, we use following theorem, which was proved in [3].

Theorem IV.2 *(Theorem 3, Corollary 2 of [3]) Let $|\psi\rangle$ be a pure m-partite stabilizer state with stabilizer S. Then the number of GHZ states, $|\Psi_m^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes m} + |1\rangle^{\otimes m})$, extractable from $|\psi\rangle$ via local unitaries is*

$$\Delta(S) = \dim(S) - \dim(S_{loc}), \qquad (3)$$

where S_{loc} is given by $S_{loc} = \sum_{\alpha=1}^{m} S_{\hat{\alpha}}$ and $S_{\hat{\alpha}} = \{g \in S | g \text{ acts trivially on } \alpha\}$.

Below we will find an upper bound for the expected value of Eq. (3) when $m = 3$, which we will then combine with the following lemmas, which imply that the number of GHZ states LU-extractable from a random m-partite stabilizer state (m fixed) concentrates tightly around its mean value when the number of qubits each party holds is large.

Lemma IV.3 *Consider the binary representation of $\mathcal{P}_n$ on $\mathbb{F}_2^{2n}$, wherein $c \in \mathcal{C}_n$ is represented by an element of $GL_{2n}(\mathbb{F}_2)$ (see, e.g., [6]). The metric of Eq (1) is given by*

$$d(c_1, c_2) = 2n - \dim \text{Ker}[\hat{c}_1 - \hat{c}_2],$$

where, e.g., $\hat{c} \in GL_{2n}(\mathbb{F}_2)$ is the representative of $c \in \mathcal{C}_n$.

This lemma, together with the fact that $\text{Rank}(\hat{c}_1 - \hat{c}_3) \leq \text{Rank}(\hat{c}_1 - \hat{c}_2) + \text{Rank}(\hat{c}_2 - \hat{c}_3)$, makes clear that the distance defined in Eq. 1 is in fact a metric.

Proof (of Lemma IV.3) To see this, note that

$$\min_{\{S_i\}} \#\{i | c_1 S_i c_1^\dagger \neq c_2 S_i c_2^\dagger\}$$
$$= \min_{\{S_i\}} \#\{i | (\hat{c}_1 - \hat{c}_2)\hat{S}_i \neq 0\} \qquad (4)$$
$$= 2n - \dim \text{Ker}[\hat{c}_1 - \hat{c}_2].$$

$\square$

Lemma IV.4 *As a function of $c \in \mathcal{C}_n$, where $n = \sum_{\alpha=1}^{m} n_\alpha$, the dimension of S_{loc}^c (defined in Theorem IV.2) of $S^c = cS_0 c^\dagger$ for some fixed stabilizer S_0 is m-Lipschitz with respect to the metric defined in Eq (1). In particular, the number of m-partite GHZ states (with $m \geq 3$) that can be LU-extracted from the state with stabilizer $S^c = cS_0 c^\dagger$, which is given by $\Delta(c) = \dim(S^c) - \dim(S_{loc}^c)$, is also m-Lipschitz.*

Proof Here, $S_{loc} = \sum_\alpha S_{\hat{\alpha}}$, where $S_{\hat{\alpha}}$ is the subset of S which acts trivially on α. The dimension of $S_{loc}^{c_1}$ is given by

$$\dim(S_{loc}^{c_1}) = \text{Rank}(\sum_\alpha \Pi_{\hat{\alpha}}\Pi_{S^{c_1}}\Pi_{\hat{\alpha}}),$$

where $\Pi_{\hat{\alpha}}$ is the projector onto the set of Paulis that act trivially on $\hat{\alpha}$ and $\Pi_{S^{c_1}}$ is the projector onto S^{c_1}. If we let $d(c_1, c_2) = l$ we see that

$$|\dim(S_{loc}^{c_1}) - \dim(S_{loc}^{c_2})|$$
$$= |\text{Rank}(\sum_\alpha \Pi_{\hat{\alpha}}\Pi_{S^{c_1}}\Pi_{\hat{\alpha}}) - \text{Rank}(\sum_\alpha \Pi_{\hat{\alpha}}\Pi_{S^{c_2}}\Pi_{\hat{\alpha}})|$$
$$\leq \text{Rank}\left[\sum_\alpha \Pi_{\hat{\alpha}}\Pi_{S^{c_1}}\Pi_{\hat{\alpha}} - \sum_\alpha \Pi_{\hat{\alpha}}\Pi_{S^{c_2}}\Pi_{\hat{\alpha}}\right]$$
$$= \text{Rank}\left[\sum_\alpha \Pi_{\hat{\alpha}}\left[\Pi_{S^{c_1}} - \Pi_{S^{c_2}}\right]\Pi_{\hat{\alpha}}\right]$$
$$\leq \sum_\alpha \text{Rank}\left[(c_1 - c_2)(\Pi_{S_0})\right]$$
$$\leq m[2\sum_\alpha n_\alpha - \dim \text{Ker}(c_1 - c_2)] = md(c_1, c_2).$$

$\square$

The following theorem shows that the average number of GHZ states which are LU-extractable from a random tri-partite stabilizer state is quite small, as long as none of the systems is larger than the other two combined.

Theorem IV.5 *Let $|\psi_{ABC}\rangle$ be a uniformly distributed tripartite stabilizer state with local dimensions such that $n_A + n_B \geq n_C, n_B + n_C \geq n_A$, and $n_A + n_C \geq n_B$. Then, the expected number of GHZ states that can be extracted from $|\psi_{ABC}\rangle$ is quite small. In particular,*

$$\mathbb{E}[\Delta|\psi_{ABC}\rangle] \leq \frac{n_C}{2^{n_A+n_B-n_C}} + \frac{n_B}{2^{n_A+n_C-n_B}} + \frac{n_A}{2^{n_B+n_C-n_A}}.$$

Proof We first express the dimension of S_{loc} using the inclusion-exclusion formula:

$$\begin{aligned}
\dim(S_{\hat{A}} + S_{\hat{B}} + S_{\hat{C}}) &= \dim(S_{\hat{A}}) + \dim(S_{\hat{B}}) + \dim(S_{\hat{C}}) \\
&\quad - \dim(S_{\hat{A}} \cap S_{\hat{B}}) - \dim(S_{\hat{A}} \cap S_{\hat{C}}) \\
&\quad - \dim(S_{\hat{B}} \cap S_{\hat{C}}). \quad (5)
\end{aligned}$$

Now note that the bipartite entanglement of the state with respect to the $A|BC$ partition is $n_B + n_C - \dim S_{\hat{A}}$, which must be no larger than n_A. Making a similar observation for the $AB|C$ and $AC|B$ partitions and adding the resulting inequalities gives

$$2(n_A+n_B+n_C) - \dim S_{\hat{A}} - \dim S_{\hat{B}} - \dim S_{\hat{C}} \leq n_A+n_B+n_C$$

so that

$$\dim S_{\hat{A}} + \dim S_{\hat{B}} + \dim S_{\hat{C}} \geq n_A + n_B + n_C. \quad (6)$$

In order to understand the behavior of the dimensions of the form $\dim S_{\hat{A}} \cap S_{\hat{B}}$, first let S^0 be a fixed stabilizer on ABC, and T_0, T_1 also be stabilizers on ABC of the same size as S^0. The Clifford elements, c_0, such that $T_0 = c_0 S^0 c_0^\dagger$ can be put in one-to-one correspondence with the c_1 such that $T_1 = c_1 S^0 c_1^\dagger$ by using some (fixed) $c_{0\to1}$ such that $c_{0\to1} T_0 c_{0\to1}^\dagger = T_1$, so that a uniform distribution of c on the Clifford group induces a uniform distribution over stabilizers of a fixed size for $c S^0 c^\dagger$. Thus, letting $S = c S^0 c^\dagger$ with c uniform on the Clifford group, we have

$$\mathbb{E}[\# S_{\hat{A}} \cap S_{\hat{B}}]$$

$$= \mathbb{E}[\#\{s \in S | s \in S_{\hat{A}} \ \& \ s \in S_{\hat{B}}\}]$$

$$= \mathbb{E}\left[\sum_{s \in S} \mathbf{1}\left[s \in T_A \ \& \ s \in T_B\right]\right]$$

$$= \mathbb{E}\left[\sum_{s_0 \in S^0} \mathbf{1}\left[c s_0 c^\dagger \in T_A \ \& \ c s_0 c^\dagger \in T_B\right]\right]$$

$$= 1 + \mathbb{E}\left[\sum_{s_0 \in S^0, s_0 \neq I} \mathbf{1}\left[c s_0 c^\dagger \in T_A \ \& \ c s_0 c^\dagger \in T_B\right]\right]$$

$$= 1 + \sum_{s_0 \in S^0, s_0 \neq I} \mathbb{E}\left[\mathbf{1}\left[c s_0 c^\dagger \in T_A \ \& \ c s_0 c^\dagger \in T_B\right]\right]$$

$$= 1 + (\# S^0 - 1)\mathbb{E}\left[\mathbf{1}\left[c s_0 c^\dagger \in T_A \ \& \ c s_0 c^\dagger \in T_B\right]\right],$$

where we have let s_0 be some fixed non-trivial element of S^0 in the last equation.

A nontrivial s_0 generates a stabilizer of dimension 1, so that the argument above implies that $c s_0 c^\dagger$ is distributed uniformly on the nontrivial Paulis, leading us to conclude that

$$\mathbb{E}[\# S_{\hat{A}} \cap S_{\hat{B}}]$$

$$= 1 + (\# S - 1) P(s \in T_A | s \in T_B, s \neq I) P(s \in T_B | s \neq I)$$

$$= (2^{n_A+n_B+n_C} - 1)\left[\frac{4^{n_C}-1}{4^{n_A+n_C}-1}\right]\left[\frac{4^{n_A+n_C}-1}{4^{n_A+n_B+n_C}-1}\right] + 1$$

$$\leq 2^{n_A+n_B+n_C}\frac{1}{4^{n_A+n_B}} + 1 = 1 + \frac{1}{2^{n_A+n_B-n_C}},$$

where T_A (T_B) denotes the subgroup of $\mathcal{P}_{n_A+n_B}$ that is trivial on A (B).

Since $\# S_{\hat{A}} \cap S_{\hat{B}}$ is at least 1 and must be a multiple of 2, this implies that $P\left[\# S_{\hat{A}} \cap S_{\hat{B}} = 1\right] \geq 1 - \frac{1}{2^{n_A+n_B-n_C}}$, which in turn implies

$$\mathbb{E}\dim S_{\hat{A}} \cap S_{\hat{B}} \leq \frac{n_C}{2^{n_A+n_B-n_C}}.$$

In a similar way we can bound $\mathbb{E}\dim S_{\hat{A}} \cap S_{\hat{C}}$ and $\mathbb{E}\dim S_{\hat{B}} \cap S_{\hat{C}}$ to find

$$\mathbb{E}\dim S_{\hat{A}} \cap S_{\hat{B}} + \mathbb{E}\dim S_{\hat{A}} \cap S_{\hat{C}} + \mathbb{E}\dim S_{\hat{B}} \cap S_{\hat{C}}$$

is no larger than

$$\frac{n_C}{2^{n_A+n_B-n_C}} + \frac{n_B}{2^{n_A+n_C-n_B}} + \frac{n_A}{2^{n_B+n_C-n_A}},$$

which can be combined with Eq. (6), Eq. (5) and Eq. (3) to give

$$\begin{aligned}
\mathbb{E}\Delta(S) &= \mathbb{E}(\dim S - \dim S_{loc}) \\
&\leq \frac{n_C}{2^{n_A+n_B-n_C}} + \frac{n_B}{2^{n_A+n_C-n_B}} + \frac{n_A}{2^{n_B+n_C-n_A}}.
\end{aligned}$$

$\square$

Theorem IV.5 can be combined with Lemma IV.4 to obtain the following theorem.

Theorem IV.6 *Let $|\psi_{ABC}\rangle$ be a uniformly distributed tripartite stabilizer state with local spaces of $n_A = \alpha n$, $n_B = \beta n$ and $n_C = n$ qubits with $\alpha, \beta > 1$, $\alpha + 1 > \beta$ and $\beta + 1 > \alpha$. Then, the number of GHZ states that can be extracted from $|\psi_{ABC}\rangle$ is quite small. In particular, letting $\delta = \max(\alpha - \beta + 1, \beta - \alpha + 1)$*

$$P\left(\Delta(\psi_{ABC}) > (\alpha + \beta + 1)\frac{n}{2^{\delta n}} + \epsilon n\right)$$

$$\leq \exp\left[-n\frac{\epsilon^2}{64}\left(\frac{1}{9(\alpha+\beta+1)}\right)\right].$$

V. MIXED BIPARTITE STATES

As a rule, the entanglement properties of mixed states can be quite difficult to understand. A mixed stabilizer

state, however, is always LU-equivalent to a tensor product of EPR pairs and a separable state, which dramatically simplifies the picture. Much like in the pure state case, the entanglement of a mixed stabilizer state can be characterized entirely in terms of the structure of its stabilizer group. The characterization we will need is given by the following theorem, which we will immediately use to get an estimate for the expected entanglement of a mixed stabilizer state.

Theorem V.1 *(Adapted from Theorem 5 of [3]) Let ρ be a mixed bipartite stabilizer state with n_A qubits on Alice's system, n_B on Bob's, and $(n_A + n_B - k)$-dimensional stabilizer S. The entanglement properties of ρ can be characterized using S', an extension of S which is the stabilizer of a purification of ρ to a system C. In particular, ρ is LU-equivalent to*

$$E(\rho) \geq \frac{\dim S'_{loc}}{2} - k + \frac{1}{2}\left[\text{Rank}(\rho_A) - n_A + \text{Rank}(\rho_B) - n_B\right] \tag{7}$$

EPR pairs together with (possibly classically correlated) local states, where $S'_{loc} = S'_{\hat{A}} + S'_{\hat{B}} + S'_{\hat{C}}$.

Proof In [3] it was shown that the number of EPR pairs between A and B that can be extracted by LU operations on a tripartite pure stabilizer state of full local ranks having stabilizer $\tilde{S}$ is exactly $\frac{1}{2}(\dim \tilde{S}_{\hat{C}} + \dim \tilde{S}_{loc} - \dim \tilde{S})$. The state we are considering, with stabilizer S', may not have full local ranks (i.e., the rank of the reduced state on A or B may be less than the dimension of that system) but a full rank state with the same entanglement can be constructed by having Alice and Bob discard any local pure states. The resulting state has local subgroup $\tilde{S}'_{loc}$ with dimension $\dim \tilde{S}'_{loc} \geq \dim S'_{loc} - (n_A + n_B - \text{Rank}\,\rho_A - \text{Rank}\,\rho_B)$ so that, noting that discarding the stabilizers of the local pure states changes the dimension of $S_{\hat{C}}$ and S by the same amount,

$$\begin{aligned} E(\rho_{S'}) &= E(\rho_{\tilde{S}'}) = \frac{1}{2}(\dim \tilde{S}'_{\hat{C}} + \dim \tilde{S}'_{loc} - \dim \tilde{S}') \\ &\geq \frac{1}{2}(\dim S'_{\hat{C}} + \dim S'_{loc} - \dim S') + \\ &\quad \frac{1}{2}(\text{Rank}\,\rho_A + \text{Rank}\,\rho_B - n_A - n_B). \end{aligned} \tag{8}$$

$\square$

Theorem V.2 *Let $\rho_{S^{n-k}}$ be the a rank 2^k stabilizer state on AB with stabilizer S^{n-k}, where A contains $n_A = n + \alpha \log n$ qubits, B has $n_B = n$ qubits and $k = \beta n$ with $0 < \beta \leq 2$. If S is uniformly distributed,*

$$\left[1 - \frac{\beta}{2}\right] n + \frac{\alpha}{2} \log n \geq \mathbb{E}[E(\rho_S)] \geq \left[1 - \frac{\beta}{2}\right] n - \frac{n^\alpha}{2^k} - \frac{1}{n^\alpha}. \tag{9}$$

Proof We first consider the state whose stabilizer is $S^0 = \langle Z_1, \ldots, Z_{n_A + n_B - k} \rangle$, where we have chosen some ordering of the qubits on AB. This

state, which we call ρ_0 is the reduced state on AB of the *pure* state on ABC with stabilizer $S^{0'} = \langle Z_i^{AB}, Z_{n_A+n_B-k+j}^{AB} Z_j^C, X_{n_A+n_B-k+j}^{AB} X_j^C \rangle$, where $i = 1 \ldots n_A + n_B - k$ and $j = 1 \ldots k$. Letting $S' = c_{AB} \otimes I_C S^{0'} c_{AB}^\dagger \otimes I_C$, and T_A (T_B) denote the subgroup of $\mathcal{P}_{(n_A+n_B)}$ that is trivial on A (B), and using the observation in the proof of Theorem IV.5 that $\dim S'_{\hat{A}} + \dim S'_{\hat{B}} + \dim S'_{\hat{C}} \geq n_A + n_B + n_C$ as well as the fact that $\dim S'_{\hat{A}} \cap S'_{\hat{B}} = 0$ (which follows from the independence of $\{cZ_i^{AB}c^\dagger, cZ_{n_A+n_B-k+j}^{AB}c^\dagger, cX_{n_A+n_B-k+j}^{AB}c^\dagger\}$), we find that

$$\dim S'_{loc} \geq (n_A + n_B + k) - \dim(S'_{\hat{A}} \cap S'_{\hat{C}}) - \dim(S'_{\hat{B}} \cap S'_{\hat{C}}).$$

Considering first the expected number of elements of $S'_{\hat{A}} \cap S'_{\hat{C}}$,

$$\mathbb{E}\#S'_{\hat{A}} \cap S'_{\hat{C}} = (2^{n_A+n_B-k} - 1)\frac{4^{n_B}-1}{4^{n_A+n_B}-1} + 1 \leq 2^{n_B-n_A-k} + 1,$$

we find that

$$\begin{aligned} -\mathbb{E}[\dim S'_{\hat{A}} \cap S'_{\hat{C}}] &\geq -\log \mathbb{E}\#S'_{\hat{A}} \cap S'_{\hat{C}} \\ &\geq -\log(1 + 2^{n_B-n_A-k}) \\ &\geq -\frac{1}{2^{n_A+k-n_B}} \end{aligned}$$

and making a similar argument for $S'_{\hat{B}} \cap S'_{\hat{C}}$ we find

$$\mathbb{E}\dim S'_{loc} \geq n_A + n_B + k - \frac{1}{2^{n_A+k-n_B}} - \frac{1}{2^{n_B+k-n_A}}.$$

Addressing the other terms in $E(\rho)$ by arguing along the lines of the proof of Theorem III.2, we find that $\mathbb{E}\,\text{Rank}(\rho_B) \geq n_B - \frac{1}{2^{(n_A-n_B)}}$ and $\mathbb{E}\,\text{Rank}(\rho_A) \geq n_B - \frac{1}{2^{n_A-n_B}}$, so that $\mathbb{E}[E(\rho_S)]$ is no less than

$$\begin{aligned} &\frac{n_A + n_B - k}{2} - \frac{1}{2^{n_A+k+1-n_B}} - \frac{1}{2^{n_B+k+1-n_A}} \\ &+ \frac{1}{2}\left[n_B - n_A - \frac{2}{2^{n_A-n_B}}\right] \\ &\geq n - \frac{k}{2} - \frac{1}{2^{k+1}}\left[\frac{1}{n^\alpha} + n^\alpha\right] - \frac{1}{n^\alpha} \\ &\geq n - \frac{k}{2} - \frac{n^\alpha}{2^k} - \frac{1}{n^\alpha}. \end{aligned}$$

The upper bound is obtained by noting that in the expression for the EPR rate given in Eq. (8), $\dim \tilde{S}'_{\hat{C}} - \dim \tilde{S}' = -2k$ while $n_A + n_B + k \geq \dim \tilde{S}'_{loc}$. $\square$

Now that we have an estimate for the expected entanglement, we would like to understand the deviations from this expected value. Once again, since the entanglement of a stabilizer state is a smooth function on the Clifford group, bounds on these deviations are essentially immediate.

Lemma V.3 *As a function of $c \in \mathcal{C}_{n_A + n_B}$, the lower bound in Eq. (7) for the entanglement of a rank 2^k stabilizer state $\rho_{cS^0c^\dagger}$ is $\frac{5}{2}$-Lipschitz with respect to the metric defined in Eq (1).*

Proof That $\dim S'_{loc}$ is 3-Lipschitz is immediate from Lemma IV.4. Since $\text{Rank} \, \rho_A$ is simply the bipartite entanglement with respect to the $A|BC$ partition, and similarly for $\text{Rank} \, \rho_B$, they are each 1-Lipschitz by Lemma III.3. As a result, the entire right hand side of Eq. (7) is $\frac{3}{2} + \frac{1}{2} + \frac{1}{2} = \frac{5}{2}$-Lipschitz. $\qquad\square$

Theorem V.4 *Let $\rho_{S^{n-k}}$ be the a rank 2^k stabilizer state on AB with stabilizer S^{n-k}, where A contains $n_A = n + \alpha \log n$ qubits and B has n qubits, and $k = \beta n$ with $0 < \beta \leq 2$. If S is uniformly distributed, then for n sufficiently large that $n \geq \max(\frac{4}{\epsilon(1-\beta/2)}, \frac{1}{2\beta} \log(\frac{4}{\epsilon(1-\beta/2)}))$ and $\frac{n}{\log n} \geq \max(\frac{\alpha-1}{2\beta}, \frac{\alpha}{\epsilon(1-\beta/2)})$, we have*

$$P\left(E(\rho_S) \notin (1 \pm \epsilon)(n - \frac{k}{2}) \right)$$
$$\leq 2 \exp\left[-\frac{n\epsilon^2 (1-\beta/2)^2}{25 \cdot 128} \frac{2n}{2n + \alpha \log n} \right].$$

Here $E(\rho_S) \notin (1 \pm \epsilon)(n - \frac{k}{2})$ is a short-hand for the union of $\{E(\rho_S) < (1-\epsilon)(n - \frac{k}{2})\}$ and $\{E(\rho_S) > (1+\epsilon)(n - \frac{k}{2})\}$.

Proof of Theorem V.4 Lemma V.3 and Theorem II.1 immediately imply that

$$P\left(E(\rho_S) < \mathbb{E}E(\rho_S) - \delta \right) \leq \exp\left[-\frac{\delta^2}{64(n_A + n_B)} \frac{4}{25} \right],$$

where the fact that $E(\rho_S)$ is $\frac{5}{2}$-Lipschitz rather than 1-Lipschitz leads to the extra factor of $(\frac{2}{5})^2$. This implies, together with Theorem V.2, that

$$P\left(E(\rho_S) < n - \frac{k}{2} - \frac{n^\alpha}{2^k} - \frac{1}{n^\alpha} - n\frac{\epsilon}{2}(1 - \frac{\beta}{2}) \right)$$
$$\leq \exp\left[-\frac{n\epsilon^2(1-\beta/2)^2}{25 \cdot 128} \frac{2n}{2n + \alpha \log n} \right]$$

which, using the conditions on n, gives us

$$P\left(E(\rho_S) < (1-\epsilon)\left[n - \frac{k}{2} \right] \right)$$
$$\leq \exp\left[-\frac{n\epsilon^2(1-\beta/2)^2}{25 \cdot 128} \frac{2n}{2n + \alpha \log n} \right]. \qquad (10)$$

Considering deviations above the mean, we find

$$P\left(E(\rho_S) > n - \frac{k}{2} + \frac{\alpha}{2} \log n + n\frac{\epsilon}{2}(1 - \beta/2) \right)$$
$$\leq \exp\left[-\frac{n\epsilon^2(1-\beta/2)^2}{25 \cdot 128} \frac{2n}{2n + \alpha \log n} \right],$$

which immediately implies, using the requirement $\frac{n}{\log n} \geq \frac{\alpha}{\epsilon(1-\beta/2)}$, that

$$P\left(E(\rho_S) > (1+\epsilon)(n - \frac{k}{2}) \right)$$
$$\leq \exp\left[-\frac{n\epsilon^2(1-\beta/2)^2}{25 \cdot 128} \frac{2n}{2n + \alpha \log n} \right]. \qquad (11)$$

Combining Eq. (11) and Eq. (10) completes the proof. $\qquad\square$

VI. DISCUSSION

We have presented a general method for bounding the deviations of random variables which are naturally defined on the Clifford group. As an illustration of this method, we characterized the typical entanglement in several sorts of random stabilizer states. We found that a random pure state has entanglement within a fraction $(1 - \epsilon)$ of the maximum possible value with probability exponentially close to 1 in the number of qubits being considered. Similarly, a random mixed stabilizer state with rank 2^k and local dimensions roughly 2^n has entanglement which is within a factor of $(1 \pm \epsilon)$ of $n - \frac{k}{2}$. This is maximal in some sense, since it is exactly the entanglement of a state with the same local dimensions and rank which is the tensor product of a maximally mixed state and EPR pairs. Finally, we showed that the average number of GHZ states that can be extracted via local unitaries from a random pure multipartite state is close to zero and that significant deviations from this mean occur only with exponentially small probability.

These results raise several questions about high dimensional states. Comparing the typical entanglement of a stabilizer state with that of a mixed state distributed according to the unitarily invariant measure considered in [19] reveals qualitatively different behavior. In particular, a typical stabilizer state of rank 2^k and local dimensions roughly 2^n will have $E_F = E_D = n - \frac{k}{2}$, whereas a typical unitarily invariant state with the same rank and dimensions will have $E_F \approx n$ and $E_D \leq n - \frac{k}{2}$ and perhaps $E_D \approx 0$. It is essential to understand what gives rise to this difference, since it is the highly entangled nature of the subspace associated with such a randomly chosen state which makes several communication protocols possible [4, 16, 19]. It would also be nice to know whether states generated by the random circuit model of [12, 13] have typical behavior more like random stabilizer states or Haar-distributed states. It seems clear that the behavior will be more like Haar distributed states when the number of gates in the circuit is allowed to grow exponentially [12], but it would be interesting to know what happens for more moderately sized circuits (see also [23]).

The dearth of stabilizer states from which a significant number of GHZ states can be LU-extracted seems to be related to the fact that random stabilizer codes often fail to achieve the capacity of a very noisy channel [11, 28, 29]. The point is that there exist stabilizer codes which allow encoded Bell pairs to be transmitted with fidelity close to 1 in a very noisy regime where the average fidelity achieved by a random stabilizer code is bounded away from 1. These "non-random" codes contain states which are LU-equivalent to a large number of GHZ states, which explains why the codes are in some sense atypical. In this case, they also have the atypical property of allowing transmission for a range of noise parameter in which a typical code does not.

Finally, we believe Theorem II.1 could be quite useful in the analysis of stabilizer codes. At the very least, due to its generality, Theorem II.1 allows one understand the typical behavior of a large class of random variables on the Clifford group without resorting to the often nasty computations of higher moments that would otherwise be necessary – given the expectation value, one need only compute the function's Lipschitz constant (which is typically quite easy) to immediately get an exponential bound on the probability of deviations from the mean.

[1] Koenraad M.R. Audenaert and Martin B. Plenio. Entanglement on mixed stabiliser states–i: Normal forms and reduction procedures. arXiv quant-ph/0505036.

[2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed state entanglement and quantum error correction. *Phys.Rev. A.*, 54:3824–3851, 1996. arXiv:quant-ph/9604024.

[3] S. Bravyi, D. Fattal, and D. Gottesman. GHZ extraction yield for multipartite stabilizer states. arXiv:quant-ph/0504208.

[4] H. Buhrman, M. Christandl, P. Hayden, H.K. Lo, and S. Wehner. On the (im)possibility of quantum string commitment. arXiv:quant-ph/0504078.

[5] Oscar Dahlsten and Martin B. Plenio. Exact entanglement probability distribution of bi-partite randomised stabilizer states. arXiv quant-ph/0511119.

[6] J. Dehaene and B. DeMoor. The clifford group, stabilizer states, and linear and quadratic operations over gf(2). arXiv quant-ph/0304125.

[7] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. arXiv quant-ph/0304127.

[8] I. Devetak, A. W. Harrow, and A. Winter. A family of quantum protocols. arXiv quant-ph/0308044.

[9] I. Devetak and P. Shor. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. arXiv quant-ph/0311131.

[10] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal. Quantum data hiding. *IEEE Trans. Inf. Theory*, 48(3):580–598, 2002. arXiv:quant-ph/0103098.

[11] D.P. DiVincenzo, P.W. Shor, and J.A. Smolin. Quantum-channel capacity of very noisy channels. *Phys. Rev. A*, 57:830–839, 1998.

[12] J. Emerson, E. Levine, and S. Lloyd. Convergence conditions for random quantum circuits. arXiv quant-ph/0503210.

[13] J. Emerson, Y.S. Weinstein, M. Saraceno, S. Lloyd, and D.G. Cory. Pseudo-random unitary operators for quantum information processing. *Science*, 302:2098–2100, 2003.

[14] D. Fattal, T. Cubitt, Y. Yamamoto, S. Bravyi, and I. Chuang. Entanglement in the stabilizer formalism. arXiv quant-ph/0406168.

[15] D. Gottesman. Stabilizer codes and quantum error correction. Caltech Ph.D. Thesis.

[16] A. Harrow, P. Hayden, and D. Leung. Superdense coding of quantum states. *Phys. Rev. Lett.*, 92:187901, 2004. arXiv:quant-ph/0307221.

[17] P. Hayden, D. Leung, P.W. Shor, and A. Winter. Randomizing quantum states: Constructions and applications. arXiv:quant-ph/0307104, 2003. Commun. Math. Phys., to appear.

[18] P. Hayden, D. Leung, and G. Smith. Multiparty data hiding of quantum information. arXiv quant-ph/0407152.

[19] P. Hayden, D. Leung, and A. Winter. Aspects of generic quantum entanglement. arXiv quant-ph/0407049.

[20] M. Ledoux. *The concentration of measure phenomenon*. American Mathematical Society, USA, 2001.

[21] E. Lubkin. Entropy of an n-system from its correlation with a k-reservoir. *J. Math. Phys.*, 19:1028–1031, 1978.

[22] B. Maurey. Constructions de suites symtriques. *C.R. Acad. Sci. Paris, Sr. A-B*, 288:679–681, 1979.

[23] Roberto Oliveira, Oscar Dahlsten, and Martin B. Plenio. Efficient generation of generic entanglement. arXiv quant-ph/0605126.

[24] E.M. Rains. Entanglement purification via separable superoperators. arXiv quant-ph/9707002.

[25] R. Raussendorf and H. Briegel. Quantum computing via measurements only. *Phys. Rev. Lett.*, 86:5188–5191, 2001.

[26] P.W. Shor. Equivalence of additivity questions in quantum information theory. arXiv quant-ph/0305035.

[27] P.W. Shor. The quantum channel capacity and coherent information. lecture notes, MSRI Workshop on Quantum Computation, 2002. http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/.

[28] P.W. Shor and J.A. Smolin. Quantum error-correcting codes need not completely reveal the error syndrome. arXiv quant-ph/9604006.

[29] G. Smith and J. A. Smolin. Degenerate coding for Pauli channels. arXiv:quant-ph/0604107.

[30] M. Talagrand. Concentration of measure and isoperimetric inequalities in product spaces. *Publications I.H.E.S.*, 81:73–205, 1995.

[31] M. Talagrand. Special invited paper - a new look at independence. *ANNALS OF PROBABILITY*, 24:1–34, 1996.

[32] B.M. Terhal and B.G.H. Vollbrecht. The entanglement of formation for isotropic states. *Phys. Rev. Lett.*, 85:2625–2628, 2000. quant-ph/0005062.

[33] A. Winter. "extrinsic" and "intrinsic" data in quantum measurements: asymptotic convex decomposition of positive operator valued measures. *Comm. Math. Phys.*, 244:157–185, 2004.

[34] W.K. Wooters. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 80:2245–2248, 1998. quant-ph/9709029.

[35] K. Zyczkowski and H.-J. Sommers. Induced measures in the space of mixed quantum states. *J. Phys. A*, 34:7111–7125, 2001. quant-ph/0012101.